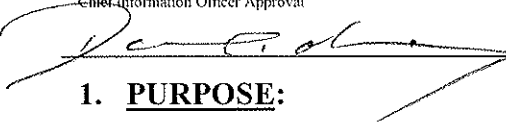




King County Information Technology Governance Policies & Standards

Title EXTERNAL NETWORK AND SYSTEMS CONNECTIVITY POLICY	Document Code No. ITE-P-07-01
Chief Information Officer Approval 	Effective Date 6-12-07

1. **PURPOSE:**

This policy establishes the rules and practices that regulate the manner in which connections are made between the King County Enterprise Network and other external Networks.

2. **APPLICABILITY:**

This policy applies to all King County Organizations and Workforce Members.

3. **REFERENCES:**

- 3.1. Countywide Information Technology Policy Governance Framework
- 3.2. King County Desktop Computer Standards
- 3.3. King County Enterprise Information Security Policy
- 3.4. King County External WAN Connectivity Standard
- 3.5. King County Password Management Policy
- 3.6. King County Information Security Best Practices Guide
- 3.7. King County Internal Network Protocol Standard
- 3.8. King County Network Infrastructure Policy
- 3.9. National Institute of Standards and Technology, U.S. Department of Commerce
- 3.10. National Security Association (NSA) Security Configuration Guides
- 3.11. NIST FIPS-140-2 Standard
- 3.12. NIST CSRC Special Publications

4. **DEFINITIONS:**

- 4.1. **Access Protection and Priority Control Mechanism (APPCM):** Examples of APPCM are access control lists, firewall rule sets and IEEE 802.11x.
- 4.2. **Agreement:** A document detailing the specifics of a relationship between parties. Examples include, but are not limited to, contract, memorandum of understanding (MOU), and memorandum of agreement (MOA) or service level agreement (SLA).

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.

- 4.3. County Enterprise Network:** The network used to conduct county business that provides transport of data within and between county facilities and other agencies of county government. This definition also refers to the network used to transport data between the county, other government agencies and the Internet. It does not refer to networks built for the sole purpose of meeting special operations needs of county business units which include, but are not limited to process control and supervisory control networks. Nor does it refer to the King County Institutional Network (I-Net), which is required to meet contractual obligations with I-Net customers and the local cable television utility.
- 4.4. Information Asset:** A definable piece of information, information processing equipment, or information system, that is recognized as "valuable" to the Organization that has one or more of the following characteristics:
- 4.4.1. Not easily replaced without cost, skill, time, resources, or a combination,
 - 4.4.2. Part of the Organization's identity, without which, the Organization may be threatened.
- 4.5. Internet:** (Upper case "I" - Internet) The largest network in the world. It is made up of more than 100 million computers in more than 100 countries covering commercial, academic and government endeavors. Originally developed for the U.S. military, the Internet became widely used for academic and commercial research.
- 4.6. Internet:** (Lower case "i" - internet) A large network made up of a number of smaller networks.
- 4.7. King County Intergovernmental Network (KC IGN):** The statewide model for connecting municipalities, counties, and the state to enable the sharing of information among employees and work groups.
- 4.8. King County Wide Area Network (KC WAN):** The network that connects King County buildings and work sites and enables the sharing of information among employees and work groups.
- 4.9. Least Privilege:** Granting a user only those access rights needed to perform official job duties.
- 4.10. Login or Logon:** The process of gaining access or signing into a computer system. The process (the noun) is a "logon" or "login," while the act of doing it (the verb) is to "log on" or "log in." If access is restricted, the logon requires Users to identify themselves by entering an ID number and/or password. Service bureaus often base their charges on the time between logon and logoff.
- 4.11. Network:** A system that transmits any combination of voice, video, and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers, and switches. In wireless systems, antennas and towers are also part of the network.

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.

- 4.12. Network Infrastructure Equipment:** Equipment that enables network connections for a facility, group, or individual to other points on the County Enterprise Network. This definition includes LAN switches, routers, and WAPs serving each facility and those used to distribute data destined to other parts of the network. It also includes appliances used to control network traffic and secure the network from unauthorized access. The appliances include, but are not limited to network traffic shapers, network firewalls, VPN concentrators, and network intrusion detection/prevention sensors.
- 4.13. Non-County User (NCU):** Any outside individual performing work for King County utilizing a personal computer, workstation, or terminal, including but not limited to: any contractor, consultant, vendor, Business Partner, or other non-county worker. Each term is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges, or benefits.
- 4.14. Organization:** Every county office, every officer, every institution, and every department, division, board, and commission.
- 4.15. Password:** A confidential sequence of characters used to authenticate an individual's identity, usually during a logon process.
- 4.16. Service Level Agreement (SLA):** A formal agreement that outlines the roles, responsibilities, procedures, and expectations shared between two parties.
- 4.17. System:** Software, hardware, and interface components that work together to perform a set of business functions.
- 4.18. Users:** Any individual performing work for King County utilizing a personal computer, workstation or terminal, including but not limited to: any employee, contractor, consultant, vendor, Business Partner or other worker. Each term is used in the general sense and is not intended to imply or convey to an individual any employment status, rights, privileges or benefits.
- 4.19. User ID or Username:** A unique code or string of characters used to identify a specific user. Also known as user accounts.
- 4.20. Workforce Member:** Employees, volunteers, and other persons whose conduct, in the performance of work for King County, is under the direct control of King County, whether or not they are paid by King County. This includes full and part time, elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to King County.

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.

5. POLICIES:

5.1. General

- 5.1.1. Network protocols used to transport traffic on the County Enterprise Network shall be restricted according to rules described in the **Internal Network Protocol Standard**.
- 5.1.2. The Access Protection and Priority Control Mechanism (APPCM) shall be appropriate for the classification of the data being processed.
- 5.1.3. Loss, compromise, or suspected loss or compromise, of the APPCM shall be immediately reported to the Office of Information Resource Management (OIRM) Help Desk.
- 5.1.4. The county shall not be liable for the accuracy of data transmitted over the Internet.

5.2. External Non-County Users

- 5.2.1. Non-county Users (NCUs), with an identifiable, justifiable, and ongoing business need may be provided access to King County's internal resources and services by way of a Network connection to the KC WAN or KC IGN. This access shall be based on formal Service Level Agreements (SLAs) between the NCU and the county, through OIRM and the department or agency providing the application's service, as outlined in the **External WAN Connectivity Standard**.
- 5.2.2. External NCU's requests for a Network connection to county services shall meet the following four (4) approval criteria before being granted:
 - 5.2.2.1. The director of the Organization that owns the county service or system has determined that sufficient direct business benefit for the county and NCU exists to justify providing a secure Network connection. The director will provide a business case justification prior to any connectivity.
 - 5.2.2.2. The county's Chief Information Security and Privacy Officer (CISPO) has determined the associated Network connection can be implemented without service disruption, constraint or violation of the integrity of the county's Networks and there is no viable method of providing the service without the Network connection. The CISPO shall generate a risk assessment to determine the acceptable level of risk and required mitigation controls.
 - 5.2.2.3. The NCU shall agree in writing to abide both in fact and spirit, to the King County Network access and security policies.
 - 5.2.2.4. The King County Chief Information Officer (CIO) has reviewed the business case documentation supplied by the organization and the risk analysis provided by the CISPO. The CIO must agree the business case

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.

for the connection outweighs the associated risk and approve the connection.

5.3. Security

- 5.3.1. King County Network Infrastructure Equipment shall be configured according to NSA standards and industry best practices for information security.
- 5.3.2. OIRM shall manage the Network connection and reserves the right to sever said connection if it negatively impacts county Network services such as, but not limited to, imposing an exceptional load on a county service or exhibiting a pattern of malicious Network traffic.
- 5.3.3. Access to the county's Networks is based on the concept of Least Privilege. Some form of Access Control Mechanism shall control all access to private, sensitive, proprietary, copyrighted or licensed information.
- 5.3.4. NCUs shall conform to the county's Network and security standards while connected to county Networks, in accordance with the **King County Enterprise Information Security Policy**.
- 5.3.5. The NCU shall be responsible for its own security requirements.

5.4. Agreements

- 5.4.1. OIRM, the requesting Organization, and the NCU shall establish an Agreement outlining the roles, responsibilities, procedures, and expectations for the daily operation, maintenance, and problem resolution, as outlined in the **External WAN Connectivity Standard**. The Agreement shall also address business services, Network management, and technical issues as they apply.
- 5.4.2. The formal Agreements between the NCUs and King County shall be reviewed by OIRM on an annual basis to ensure existing configurations and arrangements remain valid and justifiable.

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.

6. **EXCEPTIONS:**

- 6.1. Exceptions to this policy may be granted by submitting a request in writing to the **Chief Information Officer (CIO)** as described in the **Countywide Information Technology Policy Governance Framework**.
- 6.2. In each case the agency shall include such items as:
 - 6.2.1. Description of the need for the exception.
 - 6.2.2. Scope and extent of the exception.
 - 6.2.3. Quantifiable risk assessment.
 - 6.2.4. Safeguards to be implemented to mitigate quantified risks.
 - 6.2.5. Specific timeline for the exception.
 - 6.2.6. Organization within the agency requesting the exception.
 - 6.2.7. Agency director approval of the exception request.
- 6.3. Proposals for changes or request for exceptions to this policy shall be received from agencies and the **CIO** and shall be reviewed for completeness and business impacts by the **Network Policy and Standards Development Team**.

7. **RESPONSIBILITIES:**

- 7.1. The Chief Information Officer (CIO) is the approval authority for the **External Network and Systems Connectivity Policy**.
- 7.2. OIRM Network, Systems, and Operations is the steward of the network infrastructure and is responsible for providing all transport services across the KC WAN. As such, OIRM will become the owners of the network policies and standards.
- 7.3. OIRM is responsible for the operations and maintenance of all Network Infrastructure Equipment connected to the County Enterprise Network. OIRM is not responsible for Network Infrastructure Equipment that operates solely within a department **and** that OIRM has previously determined neither connects to, nor affects the operation of, the County Enterprise Network.
- 7.4. OIRM is responsible for protecting the integrity of the County Enterprise Network. To meet this responsibility OIRM shall ensure compliance with the terms detailed in the **External Network and Systems Connectivity Policy**.
- 7.5. King County departments and agencies are responsible for informing their employees of this policy.

Distribution of this document outside of King County Governmental Agencies is prohibited unless authorized in writing in advance by the Chief Information Security and Privacy Officer or their designee.

This document may be exempt from public disclosure pursuant to RCW 42.17.310(1). Requests for public disclosure of this document, or parts thereof, should be referred via the Chief Information Security and Privacy Officer for guidance and direction.